

Implementation of a Measurement-Device-Independent Entanglement Witness

Ping Xu,^{1,2} Xiao Yuan,³ Luo-Kan Chen,^{1,2} He Lu,^{1,2} Xing-Can
Yao,^{1,2} Xiongfeng Ma,³ Yu-Ao Chen,^{1,2} and Jian-Wei Pan^{1,2}

¹*Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics,
University of Science and Technology of China, Shanghai, China*

²*Synergetic Innovation Center of Quantum Information & Quantum Physics,
University of Science and Technology of China, Hefei, Anhui, China*

³*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China*
(Dated: April 17, 2014)

Entanglement, the essential resource in quantum information processing, should be witnessed in many tasks such as quantum computing and quantum communication. The conventional entanglement witness method, relying on an idealized implementation of measurements, could wrongly conclude a separable state to be entangled due to imperfect detections. Inspired by the idea of a time-shift attack, we construct an attack on the conventional entanglement witness process and demonstrate that a separable state can be falsely identified to be entangled. To close such detection loopholes, based on a recently proposed measurement-device-independent entanglement witness method, we design and experimentally demonstrate a measurement-device-independent entanglement witness for a variety of two-qubit states. By the new scheme, we show that an entanglement witness can be realized without detection loopholes.

Quantum entanglement plays an important role in the nonclassical phenomenons of quantum mechanics. Being the key resource for many tasks in quantum information processing, such as quantum computation [1], quantum teleportation [2], and quantum cryptography [3, 4], entanglement needs to be verified in many scenarios. There are several proposals to witness entanglement and we refer to Ref. [5] for a detailed review. A conventional way to detect entanglement, the entanglement witness (EW), gives one of two outcomes: “Yes” or “No”, corresponding to the conclusive result that the state is entangled or to failure to draw a conclusion, respectively. Mathematically, for a given entangled quantum state ρ , a Hermitian operator W is called a witness, if $\text{tr}[W\rho] < 0$ (output of ‘Yes’) and $\text{tr}[W\sigma] \geq 0$ (output of ‘No’) for any separable state σ . Note that there could also exist an entangled state ρ' such that $\text{tr}[W\rho'] \geq 0$ (output of ‘No’). In the experimental verification, one can realize the conventional EW with only local measurements by decomposing W into a linear combination of product Hermitian observables [5].

Focusing on the bipartite scenario, a general illustration of the conventional EW is shown in Fig. 1(a), where two parties, Alice and Bob, each receive one component of a bipartite state ρ_{AB} from an untrusted third party Eve. They want to verify whether ρ_{AB} is entangled or not, by performing local operations and measurements on $\rho_A = \text{Tr}_B[\rho_{AB}]$ and $\rho_B = \text{Tr}_A[\rho_{AB}]$. The correctness of such witness relies on implementation details of W . An unfaithful implementation of W , say, due to device imperfections, would render the witness results unreliable. For example, the measurement devices used by Alice and Bob might possibly be manufactured by another untrusted party, who could collaborate with Eve and deliberately fabricate devices to make the real implementation $W' = W + \delta W$ deviate from W , such that W' is not a witness any more,

$$\text{tr}[W'\sigma] < 0 < \text{tr}[W\sigma]. \quad (1)$$

That is, with the deviated witness W' , a separable state σ could be identified as an entangled one, which is more likely to happen when $\text{tr}[W\sigma]$ is near zero.

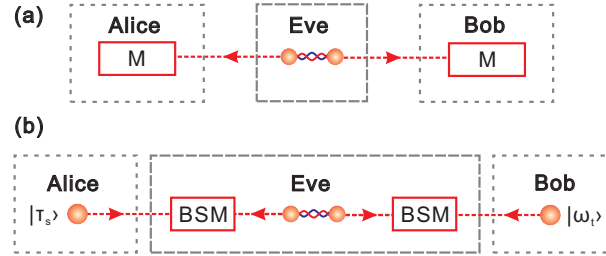


FIG. 1. (a) Conventional EW setup, where Alice and Bob perform local measurements separately and collect information to decide whether the input state is entangled or not. (b) Measurement-device-independent (MDI) EW setup, where Alice and Bob each prepare an ancillary state and a third party Eve performs Bell state measurements (BSMs) on the ancillary states and the to-be-witnessed bipartite state. Based on the choices of Alice and Bob’s ancillary states and the BSM results, they can judge whether the input state is entangled or not.

There is a strong similarity between the EW and the quantum key distribution (QKD) where an entanglement-breaking channel would cause insecurity [6]. Roughly speaking, it is crucial for Alice and Bob to prove that entanglement can be preserved in a secure QKD channel. From this point of view, there exists a correlation between the security of the QKD and the success of the EW. For the varieties of attacks in the QKD, such as time-shift attacks [7] and fake-state attacks [8], one may also find similar detection loopholes in the conventional EW process. Originating from this analogy, we construct a time-shift attack that manipulates the efficiency mismatch between detectors used in an EW process. Under this attack, any state could be witnessed to be entangled, even if the input state is separable. By this example, we demonstrate that there do exist loopholes in the conventional EW procedure.

Recently, Lo et al. [9] proposed a measurement-device-independent (MDI) QKD method, which is immune to all hacking strategies on detection. Due to the similarity between the QKD and the EW, one would also expect that there exist EW schemes without detection loopholes. Meanwhile, a nonlocal game is proposed to distinguish any entangled state from all separable states [10]. Inspired by this game, Branciard et al. [11] proposed an MDIEW method, where they proved that there always exists an MDIEW for any entangled state with untrusted measurement apparatuses.

As shown in Fig. 1(b), Alice and Bob want to identify whether a given bipartite state, prepared by an untrusted party Eve, is entangled or not without trusting measurement devices. To do so, Alice (Bob) prepares an ancillary state τ_s (ω_t) and sends it along with the to-be-witnessed bipartite state to a willing participant, who can be assumed to be Eve again in the worst case scenario. Eve performs two Bell-state measurements (BSMs) on the two ancillary states and the bipartite state. Then, she announces to Alice and Bob the results of BSMs, based on which they will witness the entanglement of the bipartite state. In the MDIEW, it is guaranteed that a separable state will never

be wrongly identified as an entangled one, even if Eve maliciously makes wrong measurements and/or announces unfaithful information [11].

In the experiment, we first show an example of the time-shift attack on the conventional EW process and demonstrate how a separable state can be falsely identified to be entangled when a large efficiency mismatch happens. Then we design and experimentally realize an MDIEW scheme to close such detection loopholes. The MDIEW is used to testify the entanglement of various bipartite states starting from maximally entangled to separable ones. Note that we use heralded single-photon sources to prepare the two ancillary states; thus, our demonstration is realized by a six-photon interferometry.

Time-shift attack, originated from quantum cryptography [7], takes advantage of the efficiency mismatch of the measurement devices. As shown in Fig. 2(a), typically two detectors are used on each side of Alice and Bob. By controlling the single-photon-counting modules (SPCMs) and coincidence gate, Eve is able to enlarge the efficiency mismatch and hence manipulate the EW result.

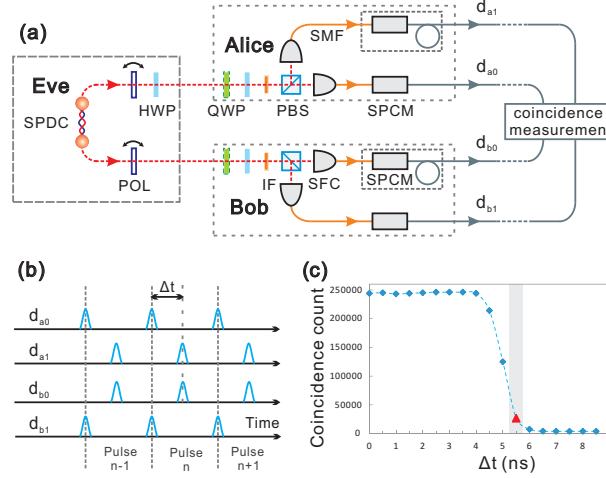


FIG. 2. Time shift attack on the conventional EW. (a) Experimental setup of the time-shift attack. Photon pairs are generated by SPDC using a femtosecond pump laser with a central wavelength of 390 nm and a repetition frequency of 80 MHz. POL: polarizer, HWP: half-wave plate, QWP: quarter-wave plate, IF: interference filter with 780 nm central wavelength, PBS: polarizing beam splitter, SFC: single-mode fiber coupler, SMF: single-mode fiber, SPCM: single-photon-counting module, some with extra internal delay lines. (b) Synchronization between SPCMs. Build-in delay lines enable Eve to shift the output signals d_{a1} and d_{b0} by Δt . (c) Coincidence count versus time delay, where the time window is set to 4 ns. All data points are measured for 2 seconds, and the time-shift attack is implemented with $\Delta t = 5.50 \pm 0.24$ ns, which corresponds to the grey area.

To implement this attack, we choose a conventional witness

$$W = \frac{1}{2}I - |\Psi^-\rangle\langle\Psi^-|,$$

for bipartite states in the form of

$$\rho_{AB}^v = (1-v)|\Psi^-\rangle\langle\Psi^-| + \frac{v}{2}(|HH\rangle\langle HH| + |VV\rangle\langle VV|), \quad (2)$$

where H (V) denotes the horizontal (vertical) polarization of the single photons and $|\Psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$ is a Bell state. By decomposing W into a linear combination of product Pauli matrices, the EW can be realized by local measurements,

$$Tr[W\rho_{AB}] = \frac{1}{4}(1 + \langle\sigma_x\sigma_x\rangle + \langle\sigma_y\sigma_y\rangle + \langle\sigma_z\sigma_z\rangle).$$

That is, to identify the entanglement, Alice and Bob just have to each analyze the qubit state in three bases separately. When the bipartite state is projected to the positive (negative) eigenstates of $\sigma_x\sigma_x$, $\sigma_y\sigma_y$, and $\sigma_z\sigma_z$, it will contribute positively (negatively) to the witness result $Tr[W\rho_{AB}]$. For example, when measuring $\sigma_x\sigma_x$, Alice and Bob will both project the input state to the eigenstates of σ_x , σ_x^+ or σ_x^- , with corresponding eigenvalues of $+1$ or -1 , respectively, and obtain probabilities $\langle\sigma_x^\pm\sigma_x^\pm\rangle$. Then the value of $\langle\sigma_x\sigma_x\rangle$ is defined as $\langle\sigma_x^+\sigma_x^+\rangle + \langle\sigma_x^-\sigma_x^-\rangle - \langle\sigma_x^+\sigma_x^-\rangle - \langle\sigma_x^-\sigma_x^+\rangle$. From Eve's point of view, she wants to convince Alice and Bob that the bipartite state is entangled, that is, $Tr[W\rho_{AB}] < 0$.

Thus, her objective is to suppress the positive contributions of $\text{Tr}[W\rho_{AB}]$, such as $\langle\sigma_x^+\sigma_x^+\rangle$ and $\langle\sigma_x^-\sigma_x^-\rangle$ for the $\sigma_x\sigma_x$ measurement, by manipulating the coincidence rate between SPCMs, equivalently enlarging the detector efficiency mismatch. In this case, from Alice and Bob's point of view, the real implemented witness W' is deviated from the desired one W , and satisfies Eq. (1). More details of the time-shift attack can be found in Appendix.

In our experiment, as shown in Fig. 2(a), by encoding qubits in the polarization of photons, the bipartite state $(|HH\rangle_{ab} + |VV\rangle_{ab})/\sqrt{2}$ is generated via spontaneous parametric down conversion (SPDC). Two adjustable POLs are used to disentangle the initial state and project it to $|HH\rangle_{ab}$ and $|VV\rangle_{ab}$ with equal probabilities, corresponding to the separable state with $v = 1$ in Eq. (2). After a 45° HWP, the to-be-witnessed two-qubit system is prepared in the state of $\rho_{AB} = (|HV\rangle\langle HV| + |VH\rangle\langle VH|)/2$. Then Alice and Bob each perform polarization analysis on a qubit from the bipartite state using waveplates, PBSs and SPCMs, and guide the electronic signals from the SPCMs into a coincidence gate.

As shown in Fig. 2(b), in the time-shift attack, Eve controls the delay lines in the detection systems and the time window of the coincidence gate, and hence, manipulates the time-dependent coincidence counting rates between detectors d_{a0} and d_{b0} , d_{a1} and d_{b1} . Hence, she can suppress the positive contributions of measurements $\langle\sigma_x\sigma_x\rangle$, $\langle\sigma_y\sigma_y\rangle$ and $\langle\sigma_z\sigma_z\rangle$. In our demonstration, by setting proper parameters, we let the positive contributions drop to 10.9(1) % of their original values. Since this attack would not affect the negative contributions of $\text{Tr}[W\rho_{AB}]$, the experimental outcomes for $\langle\sigma_x\sigma_x\rangle$, $\langle\sigma_y\sigma_y\rangle$ and $\langle\sigma_z\sigma_z\rangle$ become negative as expected. Finally, Alice and Bob obtain a witness of ρ_{AB} be $\text{tr}[W'\rho_{AB}] = -0.379(4)$, although the input state ρ_{AB} is, in fact, separable. By changing Δt to a larger value, one can even obtain a fake result for that from a maximal entangled state. Thus, a separable bipartite state could be wrongly witnessed to be entangled when Eve is able to manipulate the detection system. It is not hard to see that for any state ρ , Eve can perform a similar attack and trick Alice and Bob into thinking that it is entangled.

Note that in the original time-shift attack in the QKD [7], Eve is only able to partially control the detection efficiency by manipulating the timing of the quantum signals. In that case, Eve cannot arbitrarily enlarge the efficiency mismatch between desired and undesired detection events. In the EW case, there are two quantum signals Eve can manipulate. From our demonstration, we show that by controlling the coincident gates, Eve is able to arbitrarily decrease the coincident detection efficiency (down to 0) for any type of detection events. Thus, Eve can make the EW device output any of her desired results. From this point of view, the efficiency mismatch problem is more serious in the EW.

MDIEW is able to close all loopholes introduced by imperfect measurement devices. In this scheme, to witness entanglement existing in a bipartite state ρ_{AB} , Alice and Bob randomly choose and prepare ancillary states τ_s and ω_t from state sets $\{\tau_s\}$, $\{\omega_t\}$, respectively. By performing two BSMs on the ancillary states and the bipartite state ρ_{AB} as shown in Fig. 1(b), conditional probabilities $p(a, b|\tau_s, \omega_t) = \text{Tr}[(M^a \otimes M^b)(\tau_s \otimes \rho_{AB} \otimes \omega_t)]$ are obtained, where $M^a(M^b)$ denotes the positive operator-valued measure (POVM) element of Eve's BSM with outcome $a(b)$. The convex combination of the probabilities $p(a, b|\tau_s, \omega_t)$

$$J(\rho_{AB}) = \sum_{a,b,s,t} \beta_{s,t}^{a,b} p(a, b|\tau_s, \omega_t) \quad (3)$$

define an MDIEW. That is, ρ_{AB} is entangled while $J(\rho_{AB}) < 0$ and for any separable state σ_{AB} , we have $J(\sigma_{AB}) \geq 0$.

For any entangled state ρ_{AB} and its conventional witness W , one can construct a MDIEW in the form of Eq. (3) by decomposing W as a linear combination of product Hermitian operators, $\{\tau_s \otimes \omega_t\}$, which are used as the density matrices of the ancillary states [11]. The coefficients β depend on W , the outcomes of the BSMs, and ancillary states. We leave the calculation of β to Appendix.

Our experimental setup for MDIEW is shown in Fig. 3, where a six-photon interferometry is utilized. The to-be-witnessed bipartite state ρ_{34}^v , defined in Eq. (2), is encoded in the photon pair 3 and 4. Photon pairs 1, 2 and 5, 6 are used to prepare the ancillary input states $|\tau_s\rangle_2$ and $|\omega_t\rangle_5$, respectively. In our work, various bipartite states $\{\rho_{34}^v\}$, from maximally entangled to separable, are prepared and tested with the MDIEW. The bipartite state ρ_{34}^v is first prepared in the Bell state $|\Phi^-\rangle_{34} = (|HH\rangle - |VV\rangle)/\sqrt{2}$ via a Bell-state synthesizer [12]. As the coherence length of photons is limited by the interference filtering, two 2-mm BBO crystals in each arm result in a relative phase delay between horizontal and vertical polarization components and cause polarization decoherence. Different v can be selected by the "state selector" [13]. They satisfy the relation

$$v = \cos^2(2\theta), \quad (4)$$

where θ is the angle of the fast axis of the selector HWP.

In the experiment, eight ancillary state pairs $\{\tau_s, \omega_t\}$ are prepared. The states are encoded by tunable waveplates (one HWP sandwiched by two QWPs), which can realize arbitrary single-qubit unitary transformation. Different from direct polarization measurement in the conventional EW, the analysis of MDIEW is completed by BSMs on $\rho_3^v \otimes |\tau_s\rangle\langle\tau_s|_2$ and $\rho_4^v \otimes |\omega_t\rangle\langle\omega_t|_5$, with two, $|\Phi^\pm\rangle = (|HH\rangle \pm |VV\rangle)/\sqrt{2}$, out of four outcomes being collected.

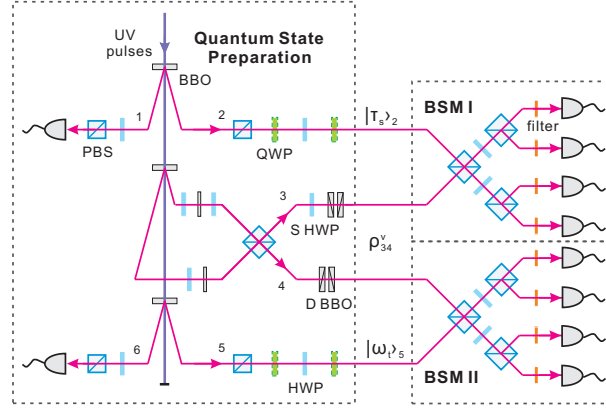


FIG. 3. Experimental setup for the MDIEW. The photon pairs are generated by type-II SPDC in 2-mm β -barium-borate (BBO) crystals. The pulsed pump laser has a central wavelength of 390 nm and a repetition rate of 76 MHz. To prepare the desired state (2), two 2-mm decoherer BBOs (D BBO) on each side with fast axis setting at 0° (up) and 180° (down) to reduce the spatial walk-off effect. By changing the angle θ of the selector HWP (S HWP), the desired state (2) is prepared with $v = \cos^2(2\theta)$. Heralded photons 2 and 5 are triggered by the detections of photon 1 and 6, respectively. Waveplates are used to rotate the polarizations to encode photons 2 and 5 to the desired states, $|\tau_s\rangle_2$ and $|\omega_t\rangle_5$. The BSM module is composed of three PBSs and two HWPs at 22.5° . All photons are filtered by narrow-band filters (with $\lambda_{FWHM} = 2.8$ nm for BSM I and $\lambda_{FWHM} = 8.0$ nm for BSM II) and then coupled into single-mode fibers which connect to SPCMs.

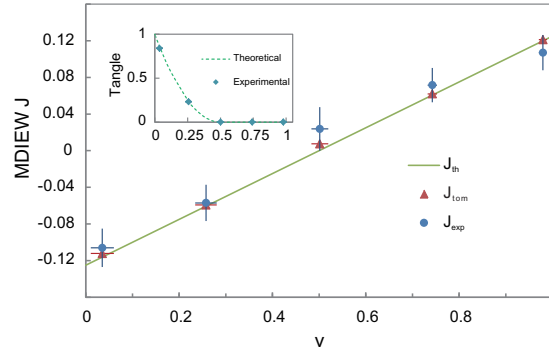


FIG. 4. MDIEW values are compared for three cases. The theoretical results (J_{th} , solid line) are calculated for the states ρ_{AB}^v with different values of v in Eq. (2). The tomography results (J_{tom} , triangle points) are evaluated for the states ρ_{34}^v after performing tomography on the to-be-witnessed bipartite state. Each point of the experimental results (J_{exp} , circular points) is measured from a 16-hour experiment. Vertical error bars indicate one standard deviation and horizontal error bars of the fitting values v from state tomography are described in Appendix. The inset shows theoretical and experimental values of tangle for input states ρ_{34}^v .

As defined in Eq. (3), we obtain the experimental results J_{exp}^v as shown in Fig. 4. In comparison, we also plot $J_{th}(\rho_{AB}^v)$ for all values of v . Recall that in the aforementioned time-shift attack demonstration, the conclusion from the conventional witness is entangled for $v = 1$, whereas here we show that our MDIEW result is 0.107 ± 0.019 and does not conclude an entangled state. One can see that our MDIEW is immune to this attack. The BSM results only provide as information whether or not the entanglement is successfully swapped. It is the ancillary states that determine whether the detection event contributes positively or negatively to the witness value defined in Eq. (3). Thus, by knowing and/or manipulating the BSM results, Eve cannot suppress the positive components of the witness, nor can she render the MDIEW to false conclusions.

Furthermore, we perform tomography on the to-be-witnessed bipartite states $\{\rho_{34}^v\}$. The results of the density matrices are shown in Appendix. The values of v are also fitted according to Eq. (4) in Appendix, which are consistent with tomography results. We evaluate the MDIEW results, Eq. (3), from the results of the state tomography J_{tom} as shown in Fig. 4. Meanwhile, to quantify the entanglement of the bipartite states $\{\rho_{34}^v\}$, we adopt the measure of tangle [14], which can be directly calculated from tomography results. When the tangle goes to zero, the bipartite state becomes a separable state. As shown in the insert of Fig. 4, no entanglement exists when v grows beyond $1/2$.

Such a phenomenon is related to the “sudden death of entanglement” [15].

In summary, we show that the conventional EW is unconfident due to the loopholes on detections. Meanwhile, as a countermeasure, we design and implement the MDIEW for the bipartite scenario, which is immune to all detection loopholes. The experimental results show that the MDIEW is practical for real-life implementation. Our method can be extended to other multipartite quantum tasks, such as quantum secret sharing.

ACKNOWLEDGMENTS

We acknowledge insightful discussions with Y.-J. Deng and Z. Zhang. This work has been supported by the National Basic Research Program of China Grants No. 2011CB921300, No. 2013CB336800, No. 2011CBA00300, and No. 2011CBA00301, the National Natural Science Foundation of China Grants, and the Chinese Academy of Sciences. P. X. and X. Y. contributed equally to this work.

Appendix A: MDIEW

Measurement-device-independent entanglement witness (MDIEW) provides means to witness entanglement of a quantum state without trusting measurement devices [11]. The idea of MDIEW is inspired from the MDI quantum key distribution (MDIQKD) [9]. As proved in Ref. [11], there always exists an MDIEW for any quantum state ρ , as one can always construct MDIEW based on the conventional witness W which exists for any quantum state (we refer to [5] for details of conventional entanglement witness). In the following, we will design an MDIEW scheme and apply it to a type of bipartite quantum states in the form of

$$\rho_{AB}^v = (1-v)|\Psi^-\rangle\langle\Psi^-| + \frac{v}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|), \quad (\text{A1})$$

with $v \in [0, 1]$ and $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. The state is entangled if $v < 1/2$, which can be witnessed by a conventional EW,

$$W = \frac{1}{2}I - |\Psi^-\rangle\langle\Psi^-|, \quad (\text{A2})$$

and its result, $\text{tr}[W\rho_{AB}^v] = (2v-1)/2$.

Practically, the conventional EW can be realized with only local measurements by decomposing W into a linear combination of product Hermitian observables. In the bipartite scenario of Alice and Bob, they only need to perform local measurements to decide the entanglement of quantum states. In contrast, MDIEW requires Alice (Bob) to prepare another ancillary state τ_s (ω_t) and perform Bell-state measurements (BSMs) on the to be witnessed state and the ancillary state. Conditioned on the measurement outcomes, a and b , MDIEW is defined as

$$J(\rho_{AB}) = \sum_{s,t} \beta_{s,t}^{a,b} p(a, b | \tau_s, \omega_t), \quad (\text{A3})$$

where the choice of the ancillary states are labeled by s and t . That is, ρ_{AB} is entangled while $J(\rho_{AB}) < 0$ and for any separable state σ_{AB} , we have $J(\sigma_{AB}) \geq 0$. Here the probabilities $p(a, b | \tau_s, \omega_t)$ are obtained from performing two BSMs on the to be witnessed state ρ_{AB} and the ancillary states τ_s and ω_t . That is,

$$p(a, b | \tau_s, \omega_t) = \text{Tr}[(M_a \otimes M_b)(\tau_s \otimes \rho_{AB} \otimes \omega_t)], \quad (\text{A4})$$

where M_a and M_b represent BSMs performed by Alice and Bob with outcome a and b , respectively. In Eq. (A3), the coefficient $\beta_{s,t}^{a,b}$ is determined by the choice of ancillary states, measurement outcomes and the conventional witness W . In the experiment, as only two $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and $|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ out of four BSM outcomes are recorded, we consider the outcomes of a and b to be $+$ and $-$, which refer to $|\Phi^+\rangle$ and $|\Phi^-\rangle$, respectively. There are four kinds of $\beta_{s,t}^{a,b}$, depending on different values of a and b . In the following, we will design $\beta_{s,t}^{a,b}$ for our MDIEW.

The case of $a = +$ and $b = +$ is considered in Ref. [11]. Decompose a conventional EW as a linear combination of product Hermitian operators, $\{\tau_s \otimes \omega_t\}$,

$$W = \sum_{s,t} \beta_{s,t}^{++} \tau_s^T \otimes \omega_t^T, \quad (\text{A5})$$

where the superscript T means matrix transpose. In the corresponding MDIEW, Alice and Bob prepare their ancillary states into $\{\tau_s\}$ and $\{\omega_t\}$, respectively. According to Eq. (A4), $p(+, +|\tau_s, \omega_t)$ is obtained by projecting the joint states $tr_B[\rho_{AB}] \otimes \tau_s$ and $tr_A[\rho_{AB}] \otimes \omega_t$ to the maximally entangled states $|\Phi_{AA}^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and $|\Phi_{BB}^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, respectively. Then it is easy to show that the relation between MDIEW and the conventional EW is

$$J(\rho_{AB}) = tr[W \rho_{AB}]/4, \quad (\text{A6})$$

which equals $(2v - 1)/8$ using Eq. (A1) and (A2).

In our work, we also consider other BSM outcomes. For example, if Alice and Bob get outcomes $a = -$ and $b = -$, then $\beta_{s,t}^{--}$ is calculated similarly as Eq. (A5) by decomposing W ,

$$W = \sum_{s,t} \beta_{s,t}^{--} \tilde{\tau}_s^T \otimes \tilde{\omega}_t^T, \quad (\text{A7})$$

where $\langle j|\tilde{\tau}|i\rangle = (-)^{i+j}\langle j|\tau|i\rangle$ and $\langle j|\tilde{\omega}|i\rangle = (-)^{i+j}\langle j|\omega|i\rangle$. By redefining the basis that W is decomposed, $\{\tilde{\tau} \otimes \tilde{\omega}\}$, the ancillary states prepared by Alice and Bob are still $\{\tau_s\}$ and $\{\omega_t\}$. In this case, $p(-, -|\tau_s, \omega_t)$ is obtained by projecting the joint states $tr_B[\rho_{AB}] \otimes \tau_s$ and $tr_A[\rho_{AB}] \otimes \omega_t$ to the maximally entangled states $|\Phi_{AA}^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ and $|\Phi_{BB}^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$, respectively.

With a similar manner, one can also decompose W for the cases of $a = +$ and $b = -$, $a = -$ and $b = +$. All the four cases of a and b are summarized in Table I.

TABLE I. Decomposition of W based on different measurement outcomes.

M_{AA}	M_{BB}	W
$ \Phi_{AA}^+\rangle = \frac{ 0\rangle \otimes 0\rangle + 1\rangle \otimes 1\rangle}{\sqrt{2}}$	$ \Phi_{BB}^+\rangle = \frac{ 0\rangle \otimes 0\rangle + 1\rangle \otimes 1\rangle}{\sqrt{2}}$	$W = \sum_{s,t} \beta_{s,t}^{++} \tau_s^T \otimes \omega_t^T$
$ \Phi_{AA}^-\rangle = \frac{ 0\rangle \otimes 0\rangle - 1\rangle \otimes 1\rangle}{\sqrt{2}}$	$ \Phi_{BB}^-\rangle = \frac{ 0\rangle \otimes 0\rangle - 1\rangle \otimes 1\rangle}{\sqrt{2}}$	$W = \sum_{s,t} \beta_{s,t}^{--} \tilde{\tau}_s^T \otimes \tilde{\omega}_t^T$
$ \Phi_{AA}^+\rangle = \frac{ 0\rangle \otimes 0\rangle + 1\rangle \otimes 1\rangle}{\sqrt{2}}$	$ \Phi_{BB}^-\rangle = \frac{ 0\rangle \otimes 0\rangle - 1\rangle \otimes 1\rangle}{\sqrt{2}}$	$W = \sum_{s,t} \beta_{s,t}^{+-} \tau_s^T \otimes \tilde{\omega}_t^T$
$ \Phi_{AA}^-\rangle = \frac{ 0\rangle \otimes 0\rangle - 1\rangle \otimes 1\rangle}{\sqrt{2}}$	$ \Phi_{BB}^+\rangle = \frac{ 0\rangle \otimes 0\rangle + 1\rangle \otimes 1\rangle}{\sqrt{2}}$	$W = \sum_{s,t} \beta_{s,t}^{-+} \tilde{\tau}_s^T \otimes \omega_t^T$

Next, we need to calculate the coefficients $\beta_{s,t}^{\pm\pm}$ and the corresponding probabilities $p(\pm, \pm|\tau_s, \omega_t)$ for given ancillary quantum states $\{\tau_s\}$ and $\{\omega_t\}$. Define $\sigma_0 = I$ and $\sigma_1, \sigma_2, \sigma_3$ to be the Pauli matrices. Then let τ_s and ω_s both be the eigenstates of σ_s with eigenvalues of 1. That is, $\tau_0 = \omega_0 = I/2$, $\tau_s = \omega_s = (I + \sigma_s)/2$ for $s = 1, 2, 3$. By decomposing W into $\{\tau_s^T \otimes \omega_t^T\}$ and $\{\tilde{\tau}_s^T \otimes \tilde{\omega}_t^T\}$, we find that the coefficients β_{st}^{ab} and the probabilities $p(a, b|\tau_s, \omega_t)$ of the two cases $++$ and $--$ are the same, and those of $+-$ and $-+$ are the same.

In the cases of $++$ and $--$, the coefficients are given by

$$[\beta_{st}^{++}] = [\beta_{st}^{--}] = \begin{bmatrix} 4 & -1 & -1 & -1 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}, \quad (\text{A8})$$

with corresponding probabilities of

$$p(+, +|\tau_s, \omega_t) = p(-, -|\tau_s, \omega_t) = \begin{bmatrix} 1/16 & 1/16 & 1/16 & 1/16 \\ 1/16 & (1-v)/16 & 1/16 & 1/16 \\ 1/16 & 1/16 & (1-v)/16 & 1/16 \\ 1/16 & 1/16 & 1/16 & (1-v)/8 \end{bmatrix}. \quad (\text{A9})$$

There are ten nonzero terms in the coefficient matrix, so ten different ancillary inputs (τ_s, ω_t) are required. In practice, it is possible to reduce the number of inputs by introducing two other states $\tau_4 = \frac{I + (\sigma_x + \sigma_y + \sigma_z)/\sqrt{3}}{2}$ and $\omega_4 = \frac{I + (\sigma_x + \sigma_y + \sigma_z)/\sqrt{3}}{2}$. In this case, we have another decomposition of W with coefficients of

$$[\beta_{st}^{++}] = [\beta_{st}^{--}] = \begin{bmatrix} 2\sqrt{3}-2 & 0 & 0 & 0 & -\sqrt{3} \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ -\sqrt{3} & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (\text{A10})$$

TABLE II. Coefficients and probabilities for MDIEW with outcomes $++$ and $--$. Note that when $\beta = 0$, the corresponding probability p is irrelevant.

	$\tau_0 = I/2$	$\tau_1 = \frac{I+\sigma_x}{2}$	$\tau_2 = \frac{I+\sigma_y}{2}$	$\tau_3 = \frac{I+\sigma_z}{2}$	$\tau_4 = \frac{I+(\sigma_x+\sigma_y+\sigma_z)/\sqrt{3}}{2}$
$\omega_0 = I/2$	$\beta = 2\sqrt{3} - 2, p = \frac{1}{16}$	$\beta = 0$	$\beta = 0$	$\beta = 0$	$\beta = -\sqrt{3}, p = \frac{1}{16}$
$\omega_1 = \frac{I+\sigma_x}{2}$	$\beta = 0$	$\beta = 1, p = \frac{1-v}{16}$	$\beta = 0$	$\beta = 0$	$\beta = 0$
$\omega_2 = \frac{I+\sigma_y}{2}$	$\beta = 0$	$\beta = 0$	$\beta = 1, p = \frac{1-v}{16}$	$\beta = 0$	$\beta = 0$
$\omega_3 = \frac{I+\sigma_z}{2}$	$\beta = 0$	$\beta = 0$	$\beta = 0$	$\beta = 1, p = \frac{1-v}{8}$	$\beta = 0$
$\omega_4 = \frac{I+(\sigma_x+\sigma_y+\sigma_z)/\sqrt{3}}{2}$	$\beta = -\sqrt{3}, p = \frac{1}{16}$	$\beta = 0$	$\beta = 0$	$\beta = 0$	$\beta = 0$

In this setting, only six ancillary sets are required (comparing to ten in the original construction). As a result, we derive the coefficients and probabilities in Eq. (A3) for outcomes $++$ and $--$, as shown in Table II.

Similarly, for the other two cases of outcomes $+-$ and $-+$, the coefficients are

$$[\beta_{st}^{+-}] = [\beta_{st}^{+ -}] = \begin{bmatrix} 0 & 1 & 1 & -1 \\ 1 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix} \quad (\text{A11})$$

with corresponding probabilities of

$$p(+, -|\tau_s, \omega_t) = p(-, +|\tau_s, \omega_t) = \begin{bmatrix} 1/16 & 1/16 & 1/16 & 1/16 \\ 1/16 & (1+v)/16 & 1/16 & 1/16 \\ 1/16 & 1/16 & (1+v)/16 & 1/16 \\ 1/16 & 1/16 & 1/16 & (1-v)/8 \end{bmatrix}. \quad (\text{A12})$$

when using the ancillary states $\tau_0 = \omega_0 = I/2$, $\tau_s = \omega_s = (I + \sigma_s)/2$ for $s = 1, 2, 3$. Similarly, we can define $\tau'_4 = \frac{I+(-\sigma_x-\sigma_y+\sigma_z)/\sqrt{3}}{2}$, $\omega'_4 = \frac{I+(-\sigma_x-\sigma_y+\sigma_z)/\sqrt{3}}{2}$ so that another decomposition of W is derived,

$$[\beta_{st}^{+-}] = [\beta_{st}^{-+}] = \begin{bmatrix} 2\sqrt{3}+2 & 0 & 0 & 0 & -\sqrt{3} \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ -\sqrt{3} & 0 & 0 & 0 & 0 \end{bmatrix} \quad (\text{A13})$$

Again, in this setting, only six measurements are required. The coefficients and probabilities of outcomes $+-$ and $-+$ are shown in Table III.

TABLE III. Coefficients and probabilities for MDIEW with outcomes $+-$ and $-+$. Note that when $\beta = 0$, the corresponding probability p is irrelevant.

	$\tau_0 = I/2$	$\tau_1 = \frac{I+\sigma_x}{2}$	$\tau_2 = \frac{I+\sigma_y}{2}$	$\tau_3 = \frac{I+\sigma_z}{2}$	$\tau'_4 = \frac{I+(-\sigma_x-\sigma_y+\sigma_z)/\sqrt{3}}{2}$
$\omega_0 = I/2$	$\beta = 2\sqrt{3} + 2, p = \frac{1}{16}$	$\beta = 0$	$\beta = 0$	$\beta = 0$	$\beta = -\sqrt{3}, p = \frac{1}{16}$
$\omega_1 = \frac{I+\sigma_x}{2}$	$\beta = 0$	$\beta = -1, p = \frac{1+v}{16}$	$\beta = 0$	$\beta = 0$	$\beta = 0$
$\omega_2 = \frac{I+\sigma_y}{2}$	$\beta = 0$	$\beta = 0$	$\beta = -1, p = \frac{1+v}{16}$	$\beta = 0$	$\beta = 0$
$\omega_3 = \frac{I+\sigma_z}{2}$	$\beta = 0$	$\beta = 0$	$\beta = 0$	$\beta = 1, p = \frac{1-v}{8}$	$\beta = 0$
$\omega'_4 = \frac{I+(-\sigma_x-\sigma_y+\sigma_z)/\sqrt{3}}{2}$	$\beta = -\sqrt{3}, p = \frac{1}{16}$	$\beta = 0$	$\beta = 0$	$\beta = 0$	$\beta = 0$

Although each of the four cases above defines an MDIEW, we can combine four of them as one to enhance the successful probability of MDIEW,

$$\begin{aligned} J &= \frac{1}{4} \sum_{a,b} \sum_{s,t} \beta_{s,t}^{a,b} p(a, b|\tau_s, \omega_t) \\ &= \frac{1}{4} \sum_{s,t} (\beta_{s,t}^{++} p(+, +|\tau_s, \omega_t) + \beta_{s,t}^{+-} p(+, -|\tau_s, \omega_t) + \beta_{s,t}^{-+} p(-, +|\tau_s, \omega_t) + \beta_{s,t}^{--} p(-, -|\tau_s, \omega_t)) \end{aligned} \quad (\text{A14})$$

By doing this, we improve the efficiency of experiments by four times comparing to the original proposal [11].

To witness entanglement for the bipartite states defined in Eq. (A1) with MDIEW defined in Eq. (A14), in total eight different ancillary state pairs should be prepared, and the results are summarized in Table IV.

TABLE IV. Our MDIEW in the form of Eq. (A14) for the bipartite states defined in Eq. (A1).

τ_s	ω_t	$\beta_{st}^{++} = \beta_{st}^{--}$	$p(+, + \tau_s, \omega_t) = p(-, - \tau_s, \omega_t)$	$\beta_{st}^{+-} = \beta_{st}^{-+}$	$p(+, - \tau_s, \omega_t) = p(-, + \tau_s, \omega_t)$
$I/2$	$I/2$	$2\sqrt{3} - 2$	$1/16$	$2\sqrt{3} + 2$	$1/16$
$\frac{I+\sigma_x}{2}$	$\frac{I+\sigma_x}{2}$	1	$(1-v)/16$	-1	$(1+v)/16$
$\frac{I+\sigma_y}{2}$	$\frac{I+\sigma_y}{2}$	1	$(1-v)/16$	-1	$(1+v)/16$
$\frac{I+\sigma_z}{2}$	$\frac{I+\sigma_z}{2}$	1	$(1-v)/8$	1	$(1-v)/8$
$I/2$	$\frac{I+(\sigma_x+\sigma_y+\sigma_z)/\sqrt{3}}{2}$	$-\sqrt{3}$	$1/16$	0	-
$\frac{I+(\sigma_x+\sigma_y+\sigma_z)/\sqrt{3}}{2}$	$I/2$	$-\sqrt{3}$	$1/16$	0	-
$I/2$	$\frac{I+(-\sigma_x-\sigma_y+\sigma_z)/\sqrt{3}}{2}$	0	-	$-\sqrt{3}$	$1/16$
$\frac{I+(-\sigma_x-\sigma_y+\sigma_z)/\sqrt{3}}{2}$	$I/2$	0	-	$-\sqrt{3}$	$1/16$

Appendix B: Time-shift attack

The idea of time-shift attack is originated from quantum cryptography [7] and takes advantage of efficiency mismatches existing in measurement devices. Inspired by this idea, we construct a time-shift attack for the conventional witness defined in Eq. (A2). Define $\sigma_0 = I$ and $\sigma_1, \sigma_2, \sigma_3$ be the Pauli matrices σ_x, σ_y , and σ_z , correspondingly. Then we can decompose W to

$$W = \frac{1}{4} \left(\sum_{i=0}^3 \sigma_i \otimes \sigma_i \right), \quad (\text{B1})$$

and the EW can be realized by local measurements,

$$\text{Tr}[W\rho_{AB}] = \frac{1}{4} (1 + \langle \sigma_x \sigma_x \rangle + \langle \sigma_y \sigma_y \rangle + \langle \sigma_z \sigma_z \rangle). \quad (\text{B2})$$

To realize the attack, we exploit the time mismatch of the two single-photon-counting modules (SPCMs) such that one detector is more efficient than the other. In this case, the real implementation (W') is deviated from the original design witness W . In the attack Eve can suppress the positive contributes of the witness result $\text{Tr}[W\rho_{AB}]$ to let the witness result $\text{Tr}[W'\rho_{AB}]$ be negative by adjusting the time mismatch. For example, when measuring $\sigma_x \sigma_x$, Alice and Bob will project the input state to the eigenstates of σ_x , that is σ_x^+ and σ_x^- , corresponding to positive and negative eigenvalue respectively, and obtain probabilities $\langle \sigma_x^\pm \sigma_x^\pm \rangle$. Then the value of $\langle \sigma_x \sigma_x \rangle$ is defined as

$$\langle \sigma_x \sigma_x \rangle = \langle \sigma_x^+ \sigma_x^+ \rangle + \langle \sigma_x^- \sigma_x^- \rangle - \langle \sigma_x^+ \sigma_x^- \rangle - \langle \sigma_x^- \sigma_x^+ \rangle. \quad (\text{B3})$$

The probabilities $\langle \sigma_x^\pm \sigma_x^\pm \rangle$ is measured from coincidence counts $N_A^\pm N_B^\pm$ of detectors, that is

$$\langle \sigma_x^\pm \sigma_x^\pm \rangle = \frac{N_A^\pm N_B^\pm}{\sum N_A^\pm N_B^\pm}. \quad (\text{B4})$$

If the positive coincidence counts are all suppressed, that is $N_A^+ N_B^+ = N_A^- N_B^- = 0$, then the outcome of $\langle \sigma_x \sigma_x \rangle$ is

$$\langle \sigma_x \sigma_x \rangle = -\langle \sigma_x^+ \sigma_x^- \rangle - \langle \sigma_x^- \sigma_x^+ \rangle = -\frac{N_A^+ N_B^-}{\sum N_A^\pm N_B^\pm} - \frac{N_A^- N_B^+}{\sum N_A^\pm N_B^\pm} = -1. \quad (\text{B5})$$

Similarly, the all the other local measurements $\langle \sigma_y \sigma_y \rangle$ and $\langle \sigma_z \sigma_z \rangle$ become -1 by suppressing positive coincidence counts, which gives a witness result of

$$\text{Tr}[W'\rho_{AB}] = -\frac{1}{2} \quad (\text{B6})$$

for any state ρ_{AB} .

In our experiment demonstration, we only suppress the positive coincidence counts to 10.9(1)% instead of neglecting all of them to make a wrong witness result of a separable state to be entangled.

Appendix C: Tomography

In the experiment, we prepare the to-be-witnessed bipartite states ρ_{AB}^v in the form of Eq. (A1) with different values v . To verify whether the prepared states ρ_{34}^v is close to the desired ones ρ_{AB}^v , their density matrices are reconstructed via quantum tomography with v controlled by the angle θ of the selector HWP, as shown in Eq. (4) in Main Text. The results of the density matrices are shown in Fig. 5. Then we fit the value v by the measured density matrixes ρ_{34}^v to the desired states ρ_{AB}^v . As shown in Eq. (A1), ρ_{AB}^v contains only real numbers, we can infer v from the real part of ρ_{34}^v , and the imaginary parts are supposed to be near zero.

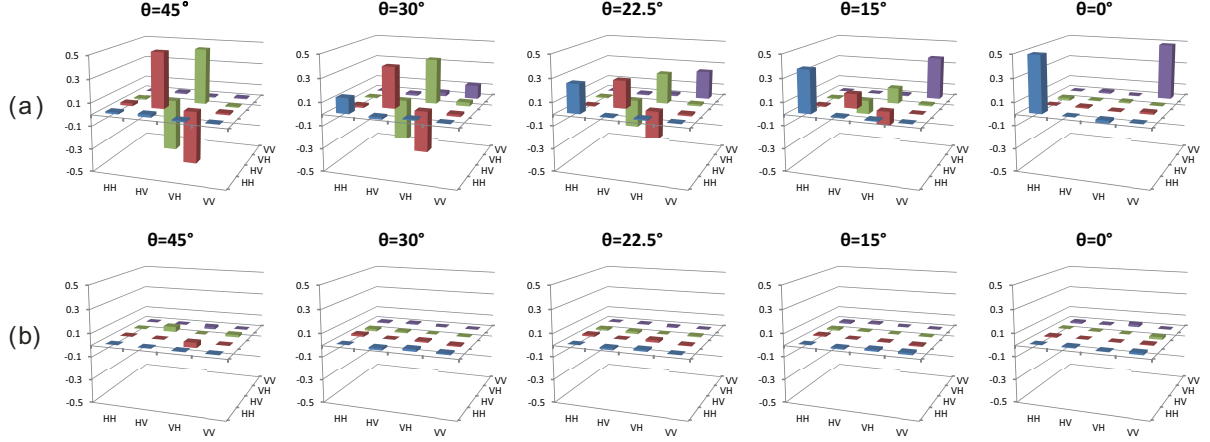


FIG. 5. Tomography of the bipartite state ρ_{34}^v . Density matrices are constructed through tomography and over 250,000 coincidence detection events are obtained for each plot. Depending on the angle θ of the state selector defined in Eq. (4) in Main Text, various states ρ_{34}^v are prepared. (a) Real part of the density matrices ρ_{34}^v . (b) Imaginary part of the density matrices ρ_{34}^v .

The parameter v can be derived from the real-part of matrix ρ_{34}^v . For each matrix elements of ρ_{34}^v , ρ_{11} , ρ_{22} , ρ_{33} , ρ_{44} , and ρ_{23} (ρ_{32} is identical to ρ_{23}), one can estimate v , as shown in Table V. Accordingly, the average value of v and its error bar are evaluated. As one can see that the experimental results agree the theoretical results well.

TABLE V. Tomography results of the input bipartite state.

θ	v_{theory}	$v_{experiment}$					\bar{v}_{exp}	$\delta\bar{v}_{exp}$	δv_{exp}
		$v_{\rho_{11}}$	$v_{\rho_{22}}$	$v_{\rho_{33}}$	$v_{\rho_{44}}$	$v_{\rho_{23}}$			
45	0	0.0196	0.0228	0.0064	0.0258	0.0290	0.0207	0.0039	0.0087
30	0.25	0.2580	0.2538	0.2426	0.2686	0.2644	0.2575	0.0045	0.0101
22.5	0.5	0.4944	0.4820	0.4824	0.5230	0.5108	0.4985	0.0081	0.0180
15	0.75	0.7298	0.7198	0.7280	0.7718	0.7620	0.7423	0.0103	0.0231
0	1	0.9680	0.9818	0.9222	0.9684	0.9822	0.9645	0.0110	0.0246

Appendix D: Tangle

To quantify the entanglement of quantum states, we adopt the measure of tangle [14]. For a 2-qubit state, ρ_{AB} , one can evaluate its tangle by the following steps.

1. Define a non-Hermitian matrix

$$R = \rho_{AB} \Sigma \rho_{AB}^T \Sigma, \quad (D1)$$

where ρ_{AB}^T is the transpose of ρ_{AB} , and the “spin flip matrix Σ ” is defined as

$$\Sigma = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}; \quad (D2)$$

2. Calculate the eigenvalues of R , and arrange them in decreasing order, $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$;
3. The concurrence of ρ_{AB} is defined as

$$C = \max\{0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}\}; \quad (\text{D3})$$

4. The tangle is defined as

$$\text{tangle} = C^2. \quad (\text{D4})$$

The tangle of a bipartite state is a measure of entanglement. If the tangle is zero, then the bipartite state ρ_{AB} must be a separable state. For states defined in Eq. (A1), we can calculate the corresponding tangle. By following the aforementioned steps, we first calculate the four eigenvalues, $0, (1-v)^2, v^2/4, v^2/4$. For $v > 2/3$, we have $v^2/4 > (1-v)^2$ and hence $\text{tangle} = C^2 = 0$. For $2/3 \geq v$, we have $v^2/4 \leq (1-v)^2$ and hence $\sqrt{(1-v)^2} - 2\sqrt{v^2/4} = 1 - 2v$. Therefore, $C = 0$ for $v \geq 1/2$ and $C = 1 - 2v$ for $v < 1/2$,

$$\text{tangle}(\rho_{AB}^v) = \begin{cases} (1 - 2v)^2 & v < 1/2 \\ 0 & v \geq 1/2. \end{cases} \quad (\text{D5})$$

The fitting value of v from state tomography and the tangles are shown in Table VI.

TABLE VI. The tangle values of the input states by tomography.

θ_{exp}	v_{theory}	v_{exp}	v_{error}	$\text{tangle}(\rho_{34}^v(\theta))$	tangle_{error}
45°	0	0.021	0.009	0.840	0.001
30°	0.25	0.257	0.010	0.233	0.001
22.5°	0.5	0.499	0.018	0	0
15°	0.75	0.742	0.023	0	0
0°	1	0.965	0.025	0	0

-
- [1] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
 - [2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
 - [3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984) pp. 175–179.
 - [4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
 - [5] O. Gühne and G. Tóth, Physics Reports **474**, 1 (2009).
 - [6] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
 - [7] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 073 (2007).
 - [8] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
 - [9] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
 - [10] F. Buscemi, Phys. Rev. Lett. **108**, 200401 (2012).
 - [11] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Phys. Rev. Lett. **110**, 060405 (2013).
 - [12] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, Nature Photonics **6**, 225 (2012).
 - [13] A. G. White, D. F. V. James, W. J. Munro, and P. G. Kwiat, Phys. Rev. A **65**, 012301 (2001).
 - [14] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
 - [15] T. Yu and J. H. Eberly, Phys. Rev. Lett. **93**, 140404 (2004).